AML & CTF INTERNAL PROCEDURES

OF

PAYTOME DMCC

(Company registration number № DMCC199423,

incorporated on the 07th of May 2024, having its registered office at Unit No: UT-11-PO-11, DMCC Business Centre, Level No 11, Uptown Tower, Dubai, United Arab Emirates;

License № DMCC-927507)

Version as of September 2024

Contents

1. General provisions

PAYTOME DMCC (hereinafter – "the Company") focuses on providing Payment Service Provider Services, in particular, Merchant Services or Payment Card Processing services for various e-commerce merchants incorporated worldwide and doing business worldwide in compliance with the applicable legal requirements and internal polices of the Company.

Merchant Services or payment card processing is the handling of electronic payment transactions for merchants. Merchant processing activities involve obtaining sales information from the merchant, receiving authorization for the transaction, collecting funds from the bank which issued the payment card and sending payment to the merchant.

The actual transfer of funds to the merchant or settlement will be performed in further way. At the end of each day, the merchant will generally review the day's sales, credits and voids. After verifying this, the merchant will close his batch, or the batch will be closed automatically. This entails closing out the days sales and transmitting the information for deposit into the Company's platform, and then to the bank. The acquiring bank routes the transaction through the appropriate settlement system against the appropriate card-issuing bank.

The card-issuing bank then sends the money back through settlement system (Visa, MasterCard etc) for the amount of the sales draft, less the appropriate "interchange fee," to the acquiring bank's account. The acquiring bank then deposits the amount, less the "discount fee" to the Company segregated client bank account. The Company then deposits the amount less the "discount fee" to the Merchant account once per 2-7 business days. Generally, within 24-72 hours, the merchants will have their money. The Company may offer some low risk Merchants "next day funding."

The settlement procedure varies on the front end depending on the program the merchant is on. A hotel, travel or car rental agency may want to get a pre-approval before the customer checks in or uses the service. The Company has many pre-built programs that any merchant can request based upon their type of business.

Internal Policies

This document sets out principles and standards for compliance and management of risks associated with financial crime in PAYTOME DMCC (hereinafter – "the Company"). The purpose of this document is to prevent the Company from being used for financial crime, to comply with all applicable requirements (including but not limited to the UAE Federal Decree- Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations - "AML-CFT Law"; Cabinet Decision No. (10) of 2019 on the Executive Regulation of Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations - "AML-CFT Decision" or "Cabinet Decision") and follow guidance provided by DMCC (including but not limited to the DMCC AML/CFT Guidelines for Financial Institutions and Designated Non-Financial Businesses and Professions dated 30th June, 2019), and to ensure that the most appropriate action is taken by the Company to mitigate the risks associated with financial crime.

This document outlines the applicable legal requirements related to detection and prevention of financial crime to which the Company must adhere, as well as internal measures which are established by the Company to ensure it complies with these legal requirements. The document

encompasses the Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), Counter-Proliferation Financing (CPF) and Sanctions Policy (collectively referred to as "the Policy") and sets the parameters for the Company in relation to AML, CTF, CPF and sanctions framework. The Policy is a complex document of the Company regulating its work on AML/CFT, and containing a description of the measures taken by the Company and undertaken procedure defined in accordance with the internal policy for AML/CFT purposes.

The basic principles of internal control for anti-money laundering, counter-terrorism financing and counter-proliferation financing are:

- Protection of the Company from the crime proceeds;
- Risk management of AML, CTF and CPF in order to minimize it;
- Independence of the Compliance officer who is in charge of ensuring the Company's compliance with the legal requirements;
- Principle of non-participation of the Company as a whole and each of its employees and officers in any operations and transactions, as well as any actions that may cause suspicion in promoting financial crime.

Scope and Application

The Policy applies to all Company employees, all units in the Company, senior management, foreign correspondents, contractors and third parties with whom Company may contract.

Company not only aims to comply with the relevant legal requirements but also mitigate and reduce the potential risk to the Company of customers using Company's products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity.

The Policy is updated at least once a year, or more frequently based on the international and local requirements and legislative changes. The Company's compliance regime includes the following:

- Appointment of a compliance officer and his/her responsibilities;
- Customer Due Diligence (Identification and Verification);
- Ongoing Customer Due Diligence and Transaction Monitoring;
- Identifying, evaluating and reporting of suspicious transactions to the FIU;
- Records Keeping (Customers and Transactions);
- Staff Training / Awareness supported by ongoing compliance training programmes;
- AML/CFT Audit Function; and
- AML/CFT Risk Management System.

Definitions

Money laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

• Placement: Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions.

• Layering: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

• Integration: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Article (2)(1) of the Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations defines 'money laundering' as follows:

「Any person, having the knowledge that the funds are the proceeds of a felony or a misdemeanour, and who willfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:

a- Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source.

b- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.

c- Acquiring, possessing or using proceeds upon receipt.

d- Assisting the perpetrator of the predicate offense to escape punishment.」

Financing of Terrorism

Financing of terrorism relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism or with the intention to dispose those funds to a terrorist group or a separate terrorist.

Articles (29)-(30) of the Federal Law no. (7) of 2014 on Combating Terrorism Crimes defines 'financing of terrorism' as follows:

Article (29)

「The following persons shall be punished by life imprisonment or a provisional imprisonment for a term not less than ten years:

1. Whoever provides, collects, prepares or maintains funds, or facilitates obtaining of the same despite of being aware that such funds would be used, partially or completely, in committing terrorist crimes.

2. Whoever provides, collects, prepares or maintains funds for a terrorist organization or person, or facilitates obtaining of the same despite of being aware of the reality of such Federal Law No. (7) of 2014 Combating Terrorism Crimes 16 terrorist organization or person.

3. Whoever gains, takes, operates, invests, possesses, transfers, deposits, saves, uses or disposes of any funds, or accomplishes any banking, financial or commercial transaction despite of being aware that such funds, whether partially or completely, are obtained from a terrorist crime, or owned by a terrorist organization, or prepared so as to finance the same .」

Article (30)

「Whoever commits the following crimes, despite of being aware that such funds, whether partially or completely, are obtained from a terrorist crime; or owned by a terrorist organization; or owned illegally by a terrorist person; or prepared so as to finance the same, shall be punished by life or provisional imprisonment for a term not less than ten years, as follows:

1. To transfer, deposit or exchange such funds so as to conceal or hide their true origin, source or illegal purpose.

2. To conceal or hide the true origin, source, location, way of disposition, movement, ownership or related rights of such funds. 3. To gain, possess, use, operate, deposit, invest, exchange or deal in such funds so as to conceal or hide their true origin, source or illegal purpose.」

Both the AML-CFT Law and the AML-CFT Decision define "funds" as "assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets."

Proliferation financing

Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Criminal conduct and Crime proceeds

Criminal property is the proceeds of criminal conduct. Crime proceeds are funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds. Criminal conduct includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion, and any other offence that is committed for profit.

Sanctions

Sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organisations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security. Sanctions can be:

a) Specific, i.e. relate to specific lists of named individuals, legal entities, organizations, vessels etc. (for example the US Department of Treasury refers to some of these entities as Specially Designated Nationals),

b) General, i.e. cover all transactions with certain countries or jurisdictions; certain transactions with countries or jurisdictions such as exports, imports or new investment, or all transactions within a certain area of activity/products (for example arms sales to a particular country).

c) Sectoral, i.e. cover certain parties in specific sectors (for example OFAC designates parties on a Sectoral Sanctions Identification List or "SSI List") but only restrict certain transactions of these designated parties.

Nominated Officer

Nominated Officer is the person within an organisation who is responsible for overseeing all activity related to anti-money laundering matters.

Suspicious Transaction Report (STR)

STR is a report made by the Company / Company's Nominated Officer to the FIU about suspicious or potentially suspicious activity, related to the money laundering, financing of terrorism or of illegal organisations.

Financial Intelligence Unit (FIU)

In the UAE, FIU is the Financial Intelligence Unit of the Central Bank of the UAE.

DMCCA

DMCC is the Dubai Multi Commodities Centre Authority, established pursuant to Law No. 4 of 2001 and by virtue of Decision No. 4 of 2002, each issued in the Emirate of Dubai, which authority has governance over the DMCC Free Zone as a Competent Authority for the purposes of Decree-Law.

2. Appointment of a compliance officer and his/her responsibilities

A Nominated Officer (also known as the MLR officer or AML Compliance Officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues. A

Company's Nominated Officer is [Name Surname].

In the absence of the Nominated Officer, Supporting Nominated Officers will take his/her place.

Company's Supporting Nominated Officer is [Name Surname].

The Company's Nominated Officers should remain up-to-date with AML/CFT rules and risks.

The Nominated Officer's responsibilities include:

i). Investigating transactions related to alleged crimes.

ii). Making sure that appropriate due diligence is carried out on customers and business partners.

iii). Reviewing and updating systems and internal procedures, making them available to all staff.

iv). Developing, implementing, monitoring, and maintaining appropriate ongoing training and awareness programmes for all staff.

v). Making sure that all business records are kept for at least 5 years from the date of completion of a transaction or of the end of the business relationship with a customer.

vi). Remaining up-to-date with AML/CFT rules and risks, reviewing new applicable legislation and updating internal Policy in line of the changes in law.

vii). Producing biannual reports to senior management concerning adherence to compliance policies, procedures, processes and controls.

viii). Receiving internal suspicious transaction/activity reporting submitted by the Company's employees, investigating the internal suspicious activity and taking appropriate action including, where appropriate, making external Suspicious Transaction Reports to the Financial Intelligence Unit of and send a copy to DMCCA.

ix). Acting as the point of contact to the DMCCA and relevant agencies concerned with AML/CFT matters, and responding promptly to any request for information made by any Competent Authority and/or Supervisory Authority.

x). Notifying DMCCA promptly regarding any communication from other authorities concerning Money Laundering and Terrorist Financing matters.

3. Responsibilities of Senior Management

A cornerstone of any sound governance structure, including those related to AML/CFT compliance, is senior management involvement and accountability. The members of the Company's senior management are ultimately responsible for the quality, strength and effectiveness of the supervised institution's AML/CFT framework, as well as for the robustness of its compliance culture.

In this regard, the Company's senior management aims to set the so-called "tone at the top," by demonstrating their commitment to ensuring an effective AML/CFT compliance programme is in place, and by clearly articulating their expectations with regard to the responsibilities and accountability of all staff members in relation to it.

Under the AML/CFT legal and regulatory framework of the United Arab Emirates, the senior management is responsible for performing certain functions related to the assessment, management and mitigation of the ML/FT risks to which their organisations are exposed, to which the Company adheres.

These responsibilities include:

- Implementation of governance, control, and operating systems. These include such elements as:
  - ✓ Appointing a qualified AML/CFT compliance officer who is approved by the relevant Supervisory Authority;
  - ✓ Ensuring a robust and effective independent audit function is in place;
  - ✓ Putting in place and monitoring the implementation of adequate management and information systems, internal controls, and policies, procedures to mitigate risks.
- Approval of internal policies, procedures and controls. These include such elements as the supervised institution's policies on overall ML/FT risk appetite and customer acceptance, as well as the framework of AML/CFT policies, procedures and controls related to areas such as:
  - ✓ Identification, assessment, understanding, and management/mitigation of ML/FT risks;
  - ✓ Performance, review and updating of customer due-diligence (including enhanced and simplified due-diligence) measures;
  - ✓ Identification and implementation of indictors to identify suspicious transactions;
  - ✓ Record retention and data protection;
  - ✓ Staff screening, training and development. •
- Oversight of the AML/CFT compliance programme. This includes such elements as:

- ✓ Reviewing and providing comments in relation to the AML/CFT compliance officer's semi-annual reports to the relevant Supervisory Authority;

- ✓ Approving the establishment and continuance of High Risk Customer Business Relationships and their associated transactions, including those with PEPs;

- ✓ Approving the establishment and continuance of Business Relationships involving high-risk countries;

- ✓ Approving the establishment and continuance of relationships with correspondent banks;

- ✓ Ensuring the adequate application of the appropriate components of the AML/CFT compliance programme to all branches and majority-owned subsidiaries, including those operating in foreign jurisdictions.

- Application of the directives of Competent Authorities. This includes such elements as:

  - ✓ Applying the directives of Competent Authorities for implementing UN Security Council decisions under Chapter VII of the Charter of the United Nations, and other related directives;

  - ✓ Implementing CDD measures defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, regarding High Risk Countries;

  - ✓ Implementing all other directives of the relevant Competent Authorities of the State, including Cabinet Decision (20) of 2019 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions, which may enter into effect from time to time.

3. Customer Due Diligence requirements

Effective Customer Due Diligence ("CDD") measures are an essential part of any system designed to prevent money laundering and financing terrorism.

CDD measures need to be carried out:

- when establishing a business relationship;
- when carried out an occasional transaction;
- where there is a suspicion of money laundering or terrorism financing; and
- where there are doubts concerning the veracity of previous identification information.

Before engaging in business relations, the Company:

i). identifies the customer and, where applicable, the customer's ultimate beneficial owner to 25% or more of controlling share by natural person, any person acting on behalf of a customer or senior management officer if cannot identify natural person.

ii). verifies the customer's identity on the basis of reliable and independent information, data or documentation using implemented KYC (Know Your Customer) program.

iii). conducts risk-rating of the customer following Risk-Based Approach with reference to a customer's type, business relationship, transaction, chosen product/service and geographical location / ties. Enhanced due diligence measures are taken when there is a suspicion of Money Laundering, Terrorist Financing activity, or where high risk circumstances are identified.

The Company maintains customer identification records including reliable documentation.

The following information and/or documentation in respect to natural persons and legal entities is requested:

a) for verification of the identity of a natural person:

i). applicant's full name (as per NID or passport);
ii). date and place of birth;
iii). nationality;
iv). physical address (residential and business / home country and UAE, if available);
v). contact details;

b) for verification of the identity of a legal entity:

i). full business name, including any trading name;
ii). registered or business address with contact details;
iii). place of incorporation or registration;
iv). current legal status;
v). valid commercial or professional license (if available) / other license if the applicant is regulated in a foreign jurisdiction outside UAE;
vi). the identity of the directors, managers, shareholders, signatories or equivalent persons with executive authority in respect of the legal entity;
vii). ultimate beneficial owners;
viii). copy of memorandum and articles of association.

The Company also conducts screening of the customers for:

i). Matches under the OFAC list;

ii). Global Affairs Canadian sanctions list;

iii). Account holders from countries listed on the Financial Action Task Force ("FATF");

iv). Account holders from countries listed on the Middle East and North Africa Financial Action Task Force ("MENAFATF");

v). Persons with significant holding, that hold over 25% equity or more in a business are now subject to AML/CTF screening;

vi). sanctions match;

vii). Visa Inc. and MasterCard Worldwide lists and Risk programs.

Special procedures apply for accounts related to and services rendered to politically exposed persons (PEPs), including senior government and political figures, particularly from certain countries, and for accounts opened by or through foreign banks and for clients from countries or industries deemed high risk.

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. The AML-CFT Law and the AML-CFT Decision define PEPs as:

"Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:

- Direct family members (of the PEP, who are spouses, children, spouses of children, parents).
- Associates known to be close to the PEP, which include: – Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. – Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP."

The Company performs enhanced due diligence and ongoing due diligence measures proportionate with the risk of the customer. High risk customers will therefore be subject to enhanced due diligence and ongoing due diligence. Ongoing due diligence processes will be applied to all existing customers within a specific period that will be determined by whether they are defined as high, medium or low.

The Company is required to keep CDD and KYC information up-to-date, so for these purposes the Company provides ongoing CDD for all clients with regularity depending on the customer's level of risk.

4. Identifying and Reporting of financial and suspicious transactions to the FIU

Within the meaning of the AML-CFT Law and its implementing AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds which a DNFBP has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing—any of the following:

- The proceeds of crime (whether designated as a misdemeanour or felony, and whether committed within the UAE or in another country in which it is also a crime);
- Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations;
- Being intended to be used in an activity related to such crimes.

It should be noted that the only requirement for a transaction to be considered as suspicious is "reasonable grounds" in relation to the conditions referenced above.

Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators, behavioural patterns, or customer due-diligence information, and it is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved.

The Company acknowledges that transactions need not be in progress or pending completion in order to be considered as suspicious. Even past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, is to be reported in accordance with the relevant requirements.

Global standards-setters have identified "red flag" indicators aimed to help detect activities related to money laundering, terrorism financing and crime proliferation financing. These "red flag" indicators suggest the likelihood of the occurrence of unusual or suspicious activity, including possible PF activities, money laundering, terrorist financing, and evasion of TFS. The Company relies on these "red flag" indicators when identifying suspicious transactions.

"Red flag" indicators include but are not limited to the following:

- Funds are sent or received via international transfers from or to higher-risk locations.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- An individual or entity's online presence supports violent extremism or radicalization.
- Irregularities during the CDD process which could include, but is not limited to:
    - ✓ Inaccurate information about the source of funds and/or the relationship with the counterparty.

- ✓ Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
- ✓ Suspicion of forged identity documents.

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- Dealings with dual-use (DUG) or controlled goods.
- Dealings with sanctioned goods or under embargo.
- Identifying documents that seem to be forged or counterfeited, or Identifying tampered or modified documents with no apparent explanation.
- Complex legal entities or arrangements that seem to be aiming to hide the UBO.
- The account holder conducts financial transactions in a circuitous manner

Following globally identified "red flags" the Company also recognizes the following Suspicion indicators:

i) Suspicion indicators for new customers include:

- Checking their identity is proving difficult;
- The customer is reluctant to provide details of his/her identity;
- There is no genuine reason for the customer to use the services of a merchant;
- Where transactions involve international transfers or foreign currency, the explanation for the business and the amount involved is unreasonable;

ii) Suspicion indicators for regular and established customers include:

- Transaction is different from the normal business of the customer;
- Size and frequency of the transaction is not consistent with the normal activities of the customer;
- Pattern of transactions has changed since the business relationship was established;

Having identified a suspicious transaction, a staff member informs the Nominated Officer using the Internal Suspicious Transaction Report. The Nominated Officer checks the Report, supplements it with his/her comments and notifies the Senior Management of the Company accordingly. The Nominated officer is also to file a written STR with the FIU promptly, without any delay; in the event the Nominated officer concludes that no external report should be made, the justification of such a decision should be recorded.

Since confidentiality is key to maintain the integrity of an investigation in respect of any Suspicious Transaction/Activity, the Company reporting a Suspicious Transaction/Activity or making a STR makes sure to comply with a prohibition to disclose to the subject of the reporting or any third party that:

- a Suspicious Transaction/Activity has been reported;
- enquiries are being made; or
- criminal investigations are being carried out as a result of an STR.

The reporting to the FYI is conducted by the Nominated officer via an online Suspicious Transaction Reporting System, which requires its users to choose from a list of suspicious indicators when filing a STR.

5. Records Keeping (Customer and Transaction)

Records keeping is an essential component of the audit trail procedures to ensure that tracing and confiscation of criminal and terrorist funds can be made.

All records and documents obtained through the due diligence measures, and the accounting files, commercial correspondence, copies of the personal identification documents, including suspicious transactions reports and the results of any analysis that was conducted are kept by the Company for the period of 5 years, depending on the depending on the circumstances, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account with the supervised institution;
- Completion of a casual transaction (in respect of a customer with whom no Business Relationship is established);
- Completion of an inspection of the records by the Supervisory Authorities;
- The issue date of a final judgment by the competent judicial authorities;
- Liquidation, dissolution, or other form of termination of a legal person or arrangement

The Company retains, among other, two main types of records:

- **Financial Transaction Records.** This category relates to operational and statistical records, documents and information concerning all financial transactions executed or processed by the supervised institution, whether domestic or international in nature.

Examples of the type of records, documents and information which the Company ensures to retain as required by legislative provisions include but are not limited to:

- ✓ Customer correspondence, requests or order forms related to the initiation and performance of all types of transactions;
- ✓ Customer payment advices, receipts, invoices, billing notifications, bills of exchange, statements of account, expense reimbursement requests or notifications;
- ✓ Credit-related correspondence and documentation, including those involving accounts receivable, cash advances or advance settlements, promissory notes, loans or guarantees and their amendments and supporting documents, disbursement or repayment records, collateral pledges, or any other form of customer credit;
- ✓ Deal tickets, trade blotters and ledgers, settlement and dividend payment records related to customer funds managed, legal structures or arrangements, or any other forms of asset trades or exchanges;
- ✓ Escrow or fiduciary account transaction records;
- ✓ Sale, purchase, lease, merger-acquisition, and similar agreements;
- ✓ Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

- **CDD Records.** This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:

    - ✓ Customer Information
    - ✓ Company Information
    - ✓ Reliance on Third Parties to Undertake CDD
    - ✓ Ongoing Monitoring of Business Relationships
    - ✓ Suspicious Transaction Reports (STRs)

Examples of the type of records, documents and information which the Company ensures to retain as required by legislative provisions include but are not limited to:

- ✓ Customer account information and files;
- ✓ Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls);
- ✓ Copies of personal identification documents, KYC and CDD (including EDD and SDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries and investigations;
- ✓ Customer risk assessment and classification records.

6. Staff information about AML-CFT procedures and Staff Training/Awareness

In order for the Company's ML/FT risk assessment and mitigation measures to be effective, the Company ensures that its employees have a clear understanding of the risks involved and can exercise sound judgment, both when adhering to the organisation's ML/FT risk mitigation measures and when identifying suspicious transactions.

The Company maintains an ongoing employee training programme so that the staff is adequately trained in KYC procedures and that the staff is aware of different possible patterns and techniques of money laundering which may occur in their everyday business.

Training requirements have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers/Merchants. New staff is educated in the importance of KYC policies and the basic requirements at the Company. Training is given to all staff members upon commencement of taking on the position in the Company (or at least within 60 days of commencement of employment) and on regular occasions afterwards (at least once a year).

Staff members who deal directly with customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities or sanctions violation typologies.

Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Employees are kept informed of up-to-date risk vulnerabilities, including information on current AML/CFT prevention techniques, methods and trends.

Employees are properly instructed to detect suspicious customers and transactions and notify the Nominated Officer about such suspicions as soon as possible. The appropriate Suspicious Transaction Report Form which is to be used by staff can be found in Annex 1.

Training covers the following issues:

- The law relating to financial crime;
- Risks associated with the financial crime threat to the company
- (see, for example, www.egmontgroup.org);
- Identity and responsibilities of the Nominated Officer;
- Internal policies and procedures put in place;
- Customer Due Diligence/Enhanced due diligence monitoring measures;
- Suspicious activity – what to look out for;
- How to submit an internal Suspicious Transaction Report to the Nominated Officer;
- Record-keeping requirements;
- Possible sanctions violation – what to look out for;

The Nominated Officer keeps a log of all training which is provided to staff members. All staff are required to sign the training log where required to confirm that they have received training.

The Nominated Officer circulates to all staff other materials to heighten awareness of anti-financial crime issues.

The Company will use available international training programs and offered training sessions for regular updates of internal training programs and others learning possibilities which are offered by well-known and reputable organisations (for example ACCP, ACAMS, ICA).

Records including dates of training sessions, a description of training provided and names of the employees that received training are kept by the Company for a period of 5 years from the date on which training was received.

7. AML/CFT Audit Function

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework.

An AML audit serves is an integral part of the Company's business by helping to protect the Company from being and unintentional conduit for money laundering and fraud.

The audit is a systematic check of the Company's AML/CFT risk assessment and the Company's AML/CFT program by a suitable qualified person (the auditor). The end result is a written report on whether the Company meets minimum requirements for the Company's AML/CFT risk assessment and the Company's AML/CFT program, and whether the AML/CFT program is adequate and effective throughout a specified period, and any changes are required.

Audit of the Program includes whether it complies with all of the legislative obligations, whether internal policies, procedures and controls are based on the AML/CFT risk assessment, are adequate, and have operated effectively throughout the period.

The Company ensures that the periodic inspection and testing of all aspects of its AML/CFT compliance programmes, including ML/FT risk assessment and mitigation measures, and customer due diligence policies, procedures and controls are conducted on a regular basis.

8. AML/CFT Risk Management System

The Company adheres to the Risk-based Assessment approach when working with partners and customers.

Proper identification of risk factors is crucial to the effective implementation of a risk-based approach to assessing and mitigating ML/FT risk. Identified risk factors are used for the accurate categorisation of risks, as well as for the application of appropriate mitigation measures at both the enterprise and the customer level. At the enterprise level, this includes adopting and applying adequate policies, procedures, and controls to business processes. At the customer level, this includes assigning appropriate risk classifications to customers and applying due diligence measures that are commensurate with the identified risks. The Company has both in place to effectively exercise Risk-based approach in course of its operations.

i) Customer risk

Enterprise-level, or business-level, risk factors in regard to customers relates to broad categories of customers. The various types and the extent of enterprise-level customer risk to which the Company may be exposed are handled at different levels of AML/CFT resources, with different mitigation strategies being employed.

The Company considers the following risk factors, among others:

- **Target markets.** The risks related to retail customers and their product/service needs may be different from those related to high net worth or corporate customers and their respective product/service needs. Likewise, the risks associated with resident customers may be different from those associated with non-resident customers.

- **Size, homogeneity and growth rates of customer base.** The Company is prepared to implement changes into its internal procedures depending on the parameters of its customer base as it understands that supervised institutions with small, homogenous customer bases may face different risks from those with larger, more diverse customer bases, as well as entities targeting high levels of market share growth may face different customer risks than those with less aggressive growth targets or more established customer bases.

- **Business model and strength of relationship.** The Company adopts agile approach understanding that there can be different levels of customer ML/FT risk, depending on how the business models impact the strength of customer relationships (for instance, occasional, or one-off interactions with customers).

- **IT infrastructure and management information systems (MIS) capabilities.** The Company considers how well its technical infrastructure, including data management and management information reporting capabilities, are suited to the ML/FT risk mitigation requirements of the different types of customers it deal with, particularly in respect of the size and growth dynamics of their customer base.

Special attention is given by the Company to the critical role that **customer-specific, or relationship-specific risks.**

The customer-specific risks that the Company considers include (but are not limited to):

- **Complexity and transparency.** The Company acknowledges that business relationships with complex legal, ownership, or direct or indirect group or network structures, or with less transparency with regard to Beneficial Ownership, effective control, or tax residency, may pose different ML/FT risks than those with simpler legal/ownership structures or with greater transparency.

- **Regulation/supervision.** The Company takes into account that it may face different risks from customers involved in highly regulated and supervised activities than from those involved in activities that are unregulated, and attributed cases may require different level of scrutiny by the Company.

- **Associations or linkages.** The Company acknowledges that customers associated with higher-risk persons or professions (for example, foreign PEPs and/or their companies), or those linked to sectors associated with higher ML/FT risks, may expose it to different levels of risk than customers associated with lower-risk persons and professions, and such higher-risk partners or customers should undergo enhanced due diligence on both onboarding stage and further ongoing cooperation.

ii) Geographic risk

The Company also considers geographic risk factors at both the enterprise and customer-specific levels.

Examples of some of these factors include (but are not limited to):

- **Regulatory/supervisory framework.** Countries with stronger AML/CFT controls present a different level of risk than countries with weaker regulatory and supervisory frameworks.

- **International Sanctions.** The Company considers whether the countries or jurisdictions it deals with are the subject of international sanctions, such as targeted financial sanctions, OFAC sanctions, or EU restrictive measures, that could impact Company's ML/TF risk exposure and mitigation requirements.

- **Reputation.** The Company considers whether the countries or jurisdictions it deals with are associated with higher or lower levels of ML/FT, corruption, and transparency (particularly as regards financial and fiscal reporting, criminal and legal matters, and Beneficial Ownership, but also including such factors as freedom of information and the press).

- **Consistency with customer's profile.** The Company considers whether the countries or jurisdictions that are associated with a customer are consistent with the customer's profile, including principal residential or operating locations and the type of business or professional activities with which the customer is involved.

iii) Product-, Service-, Transaction-Related Risk

The ML/FT risks associated with product, service, and transaction types influence the kinds and levels of AML/CFT resources and mitigation strategies which supervised institutions require. When identifying and assessing these risks, the Company considers both the enterprise-level risks and customer-specific or Business Relationship risks in relation to the particular circumstances.

Examples of factors that the Company considers, among others, are:

- **Typology.** The Company considers whether the product, service, or transaction type is associated with any established ML/FT typologies.

- **Complexity.** Products, services, or transaction types that favour complexity, especially when that complexity is excessive or unnecessary, can often be exploited for the purpose of money laundering and/or the financing of terrorism or illegal organisations. The Company considers conceptual, operational, legal, technological and other complexities of the product, service, or transaction type. The Company acknowledges that those with higher complexity or greater dependencies on the interactions between multiple systems and/or market participants may expose it to different types and levels of ML/FT risk than those with lower complexity or with fewer dependencies on multiple systems and/or market participants.

- **Transparency and transferability.** Situations that favour anonymity can often be exploited for the purpose of ML/FT. The Company considers the level of transparency and transferability of ownership or control of products, services, or transaction types, particularly in respect of the ability to monitor the identities and the roles/responsibilities of all parties involved at each stage. Special attention is given to products, services, or transaction types in which funds can be pooled or comingled, or in which multiple or anonymous parties can have authority over the disposition of funds, or for which the transferability of Beneficial Ownership or control can be accomplished with relative ease and/or with limited disclosure of information. The Company also considers in this regard are market size, registration or documentation requirements, operational controls, and accessibility.

- **Size/value.** The Company acknowledges that products, services, or transaction types with different size or value parameters or limits may pose different levels of ML/FT risk. So, the Company also considers whether the products, services, or transaction types it deals with have adequate controls and/or management reporting thresholds with regard to intrinsic size or value, as well as in regard to changes in size or value patterns over time.

iv) Channel-Related Risk

Different channels for the acquisition and management of customer relationships, as well as for the delivery of products and services, entail different types and levels of ML/FT risk. The Company identifies and evaluates these risks at both the enterprise-wide and the customer-specific levels. When evaluating channel-related risk, the Company pays particular attention to those channels, whether related to customer acquisition and/or relationship management, or to product or service delivery, which have the potential to favour anonymity. Among others, these may include non-face-to-face channels, such as internet-, phone-, or other remoteaccess services or technologies; the use of third-party business introducers, intermediaries, agents or distributors; and the use of third-party payment, money/value transfer, or other transaction intermediaries.

iv) Other Risk Factors

Given the ever-evolving nature of ML/FT risks, new risk factors are constantly emerging, while existing ones may change in their relative importance due to legal or regulatory developments, changes in the marketplace, or as a result of new or disruptive products or technologies. For this reason, no list of risk factors can ever be considered as exhaustive. In order to ensure, therefore,

that the Company is in a position to implement risk assessment models and mitigation measures that are appropriate to its particular circumstances, the Company takes into consideration the results of the annual NRA as well as considers consulting publications from official sources on a regular basis, including those of the relevant Supervisory Authorities, the FIU, international organisations such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others.

Examples of some of the types of additional risk factors which the Company considers in identifying and assessing its ML/FT risk exposure include, but are not limited to the following:

- **Novelty/innovation.** The Company considers the depth of experience with and knowledge of the product, service, transaction, or channel type, at both the enterprise-level (for example, with regard to operational risk) and the customer-specific level. Products, services, transaction, or channel types that are new to the market or to the enterprise may not be as well understood as, and may therefore pose a different level of ML/TF risk than, more established ones. Likewise, products, services, transaction, or channel types which are unexpected or unusual with respect to a particular type of customer may indicate a different level of potential ML/FT risk exposure than would more traditional or expected product, service, transaction, or channel types in regard to that same type of customer.

Cyber security/distributed networks. The Company evaluates the degree to which its operational processes and/or its customers expose them to the risk of exploitation for the purpose of professional third-party money laundering and/or the financing of terrorism or of illegal organisations, through cyber attacks or through other means, such as the use of distributed technology or social networks. An example of such a risk is the recent dramatic increase in the global incidence of so-called CEO fraud, in which fraudsters troll companies with phishing e-mails that are purportedly from the CEO or other senior executives, and attempt to conduct fraudulent transactions or obtain sensitive data that can be used for criminal purposes.

A "risk rating" is given to each criterion and each partner and customer accordingly:

Risk Ranking	Grading
L	Low-risk
M	Meidum-risk
H	High-risk
P	Prohibited

Risk Mitigation Strategies

The Company has implemented the following risk mitigation strategies:

1. Customer Identification, Due Diligence and Know Your Customer. The Company has implemented a Customer Identification Program (CIP) that enables personnel to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. In general, this program:

1.1. Identifies and verifies the identity of each customer on a timely basis;

1.2. Takes reasonable risk based measures to identify and verify the identity of any beneficial owner;

1.3. Obtains appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions;

1.4. Assesses the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. This due diligence process includes:

1.4.1. A standard level of due diligence that is applied to all customers when initiating or continuing a relationship, such as:

1.4.1.1. Evaluating the nature of the relationship. As an example, determining the length of a customer's relationship with the Company, the products and services provided to a customer, and the manner in which a customer was referred to the Company. The nature of a customer's relationship may serve to mitigate or to increase the overall risk indicators described below.

1.4.1.2. Identifying high risk geographies, including customers located in or conducting business transactions in High Risk Money Laundering and Related Financial Crime Areas; and

1.4.1.3. Identifying high risk entities, banking functions and transactions (refer to the High Risk Entities subtopic below).

1.4.2. The standard level being reduced in recognized lower risk scenarios, such as:

1.4.2.1. Publicly listed companies subject to regulatory disclosure requirements;

1.4.2.2. Other financial institutions (domestic or foreign) subject to an AML regime consistent with all AML recommendations;

1.4.2.3. Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds; or

1.4.2.4. Transactions involving the minimum amounts for particular types of transactions (e.g. small insurance premiums).

1.4.3. The standard level being increased with respect to customers that are determined to be of higher risk due to the nature of their activities which may require increased monitoring. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as correspondent Company in relationships. These enhanced due diligence procedures include, but are not limited to:

1.4.3.1. Increased awareness by Company personnel of higher risk customers and transactions within business lines across the Company;

1.4.3.2. Increased levels of the Company's CIP, Know Your Customer (KYC), and enhanced due diligence;

1.4.3.3. Appropriate additional documentation is obtained to confirm the identity and lawful business activities of a customer;

1.4.3.4. Escalation for approval of the establishment of an account or relationship;

1.4.3.5. An understanding of the normal and expected transactions of a customer, including increased monitoring of transactions;

1.4.3.6. Increased levels of ongoing controls and frequency of reviews of relationships; and

1.4.3.7. Reporting of suspicious activities in compliance with existing reporting requirements.

2. Refer to the Customer Identification Program Policy and Know Your Customer Policy topics of this policy for detailed guidance.

2.1. Monitoring of Customers and Transactions. The degree and nature of monitoring performed by the Company is based upon its size, the AML risks that the Company has identified, the monitoring method being utilized (manual and/or automated), and the type of activity under scrutiny. Not all transactions, accounts or customers are monitored in the same way.

2.2. The degree of monitoring is based on the perceived risks associated with a customer, the products or services being used by the customer, and the location of the customer and the transactions. In any respect, such monitoring is appropriately documented. The principal of the Company's risk based monitoring system is to respond to enterprise wide issues based on the Company's analysis of its major risks. Monitoring under this risk based approach allows the Company to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose are reviewed on a regular basis to determine adequacy for the risk levels established. In addition, adequacy of any systems and processes are assessed on a periodic basis by Senior Management and appropriately documented. Refer to the appropriate topics of this policy for detailed guidance with respect to the monitoring of customers and transactions.

2.3. Suspicious Transaction Reporting. The regulatory and legal requirement to report suspicious transactions or activity by the Company provides federal authorities the ability to utilize such financial information to combat money laundering, terrorist financing and other financial crimes. When a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made by the Company. Therefore, a risk based approach for the reporting of suspicious activity under these circumstances is not applicable.

2.4. However, a risk based approach is appropriate for the purpose of identifying suspicious activity (such as directing additional resources at those areas the Company has identified as higher risk). In the same respect, the Company uses information provided by state and federal authorizes to enhance its approach for identifying suspicious activity. In addition, Management should always periodically assesses the adequacy of the Company's system employees training and assessment for identifying and reporting suspicious transactions.

2.5. Training and Awareness. The Company provides its employees with AML Program training that is appropriate and proportional with regard to money laundering and terrorist financing for their respective positions. This enterprise wide effort provides all

relevant employees with general information on AML laws, regulations and internal policies that is:

2.5.1. Tailored to the appropriate staff responsibility (e.g. customer contact or operations);

2.5.2. At the appropriate level of detail (e.g. front line personnel, complicated products or customer managed products);

2.5.3. At a frequency related to the risk level of the business line involved; and

2.5.4. Tested to assess knowledge commensurate with the detail of information provided.

Annex 1: Internal Suspicious Transaction Report Format

SAR No.: ……/ ……..

Particulars	Remarks
Date:	
ID of the Customer:	
Name/address of the Customer:	
Telephone No. of the Customer:	
Nature of suspicious activity:	
Give the full details of suspicion: [Include detail of transactions and identity checks.]	
Attach any relevant documents: 1. Transaction receipts 2. Proof of ID and Address 3. Sanctions list checks	
Name of the Reporting Officer:	
Signature of the Reporting Officer:	
Refer to FIU: [To be completed by the Nominated Officer]	
Do not refer to FIU: Reason for decision: [Give details]	
Signature of the Nominated Officer	
Date referred to the Nominated Officer's Decision:	